

A method and an electrical device for efficient multi-rate pseudo random noise (PN) sequence generation.

5 The present invention relates to an electrical device for  
generating a multi-rate PN sequence comprising:

- sequence generation means adapted to output a plurality of sequence values on the basis of a step control signal ( $S_t$ ).

10

The present invention also relates to a method of generating a multi-rate PN sequence comprising the step of:

- generating a plurality of sequence values on the basis  
15 of a step control signal ( $S_t$ ).

Pseudo random noise sequences (PN sequences) are used in many cryptographic and communications applications to provide randomly appearing symbols. Typically, cryptographic applications are methods to provide confidentiality of transmitted information through the use of stream ciphers. In communications systems PN sequences may e.g. be used as spreading sequences in spread-spectrum communications systems where they determine the hop sequence and/or the direct spreading sequence.

In general a receiver of a spread-spectrum communications system will receive a digital signal/bit stream transmitted over a single carrier frequency which is combined from a digital signal/bit stream containing information such as a digitized voice and from a PN sequence used to code or encrypt the transmission. Typically, the length of the PN sequence stream is much larger than the length of the information stream thereby,

complicating identification of ciphers containing the actual information.

09742711-120000  
In the prior art, the PN sequences are sometimes derived  
5 by using a maximal length polynomial. Constructions, whether hardware or software implemented, which form PN sequences, in this manner are sometimes referred to as m-sequence generators. It is well known that the randomness  
10 properties of the sequences generated by the m-sequence generators are very limited as a result of a linear relationship between the symbols of the sequence. This enables prediction of the next symbol given sufficiently many but small number of previous symbols. This is not desirable in various applications, and hence there is a  
15 need for efficient techniques to enhance the unpredictability.

Clock control of the m-sequence generator is a well-known method that can be used to increase the unpredictability  
20 of m-sequence generators. The most frequent method of clock control is that of introducing two modes of operation in an m-sequence generator. In one mode the generator outputs the previously produced symbol, and in the other mode the generator outputs the next symbol from  
25 the m-sequence. The current mode can advantageously be determined by another PN sequence. Output bits generated by a clock controlled m-sequence generator form the PN sequences which are used, inter alia, to encrypt or spread an information signal.

30 The abovementioned method of clock control, also sometimes referred to as the stop-and-go method, is especially used in hardware realisations where it is easy to implement this stop-and-go method. However, the  
35 randomness properties of the resulting sequence, although less predictable, are impaired by the fact that the

( (1,2)-step) scheme, i.e. a basic m-sequence generator generates the next symbol (mode 1) or the symbol after the next symbol (mode 2), instead of the stop-and-go  
5 scheme. When implementing such a clock controlled generator, the basic m-sequence generator is required to produce symbols at twice the rate of the rate needed for output symbols. Known solutions for this depend on the  
10 use of a higher internal clock rate for the basic m-sequence generator or on the use of a very complex hardware realisation of clock controlled basic m-sequence generators.

15 EP 0905611 A2 discloses a pseudorandom number generating  
method and pseudorandom number generator where a selector  
selects a pseudorandom number  $X_j$  (a single bit) from  
either one of two function generator outputs on the basis  
of a previous pseudorandom number  $X_{j-1}$ . The two function  
20 generators output data composed of a plurality of bits  
corresponding to state data held in a register.

Another selector selects one of the data outputs of the function generators on the basis of the previous pseudorandom number  $X_{j-1}$  and stores this in the register as state data.

The abovementioned pseudorandom generator in EP 0905611 A2 does not disclose a clock controlled multi-rate generator and is subject to the abovementioned deterioration of unpredictability, since a clock rate twice as high as the needed output rate is needed because only one symbol is output at a time.

35 US 5,878,075 discloses a method of and an apparatus for  
generating a pseudorandom noise sequence (PN sequence),

where a bit sequence of pseudorandom numbers is augmented by a extra bit in order to comply with the Interim Standard IS-95 for implementation of CDMA (Code Division Multiple Access), where a sequence of  $2^{15}$  bits is  
5 required.

An object of the invention is to provide an electrical device for efficient multi-rate PN sequence generation of simplified construction which is capable of generating  
10 one or more m-sequences at a multi-rate.

This object is achieved by an electrical device of the aforementioned type, said the device further comprising:  
• selection means adapted to select one of said plurality  
15 of sequence values on the basis of a select value ( $M_t$ ),  
and  
• step control means adapted to provide the step control signal ( $S_t$ ).

20 Hereby, a flexible, efficient and cryptographically more secure generation of sequences of pseudorandom ciphers is provided, which avoids the use of multiple system clocks and only requires little additional hardware and thereby little additional power consumption.

25 In accordance with one embodiment of the device according to the invention, the select value ( $M_t$ ) is provided on the basis of a clock control value/signal ( $C_t$ ) and a previously generated select value ( $M_{t-1}$ ).

30 In accordance with another embodiment, the step control signal ( $S_t$ ) is provided on the basis of a clock control value/signal ( $C_t$ ) and a previously generated select value ( $M_{t-1}$ ).

35

In a preferred embodiment, the plurality of sequence values is two, the step control signal ( $S_t$ ) is calculated as  $S_t = (C_t + M_{t-1}) \text{ DIV } 2$  and the select value ( $M_t$ ) is calculated as  $M_t = (C_t + M_{t-1}) \text{ MOD } 2$ .

5

Hereby a (1,2)-step clock controlled m-sequence generator is provided with very little additional hardware.

Alternatively, the plurality of sequence values is four and the select value ( $M_t$ ) is calculated as  $M_t = (C_t + M_{t-1}) \text{ MOD } 4$  and the step control signal ( $S_t$ ) is calculated as  $S_t = (C_t + S_t) \text{ DIV } 4$ .

10

Hereby an efficient (1,2,3,4)-step clock controlled m-sequence generator is provided.

15

In general any N-step clock controlled m-sequence generator may be provided according to this invention, where  $N \geq 2$ . Accordingly the select value ( $M_t$ ) may be calculated as  $M_t = (C_t + M_{t-1}) \text{ MOD } N$  and the step control signal ( $S_t$ ) may be calculated as  $S_t = (C_t + S_t) \text{ DIV } N$ .

20

Hereby an efficient N-step clock controlled m-sequence generation method is provided which an unpredictability that grows with N.

25

In an embodiment the sequence generation means is a windmill polynomial sequence generator.

30 In yet another embodiment the sequence generation means comprises:

- a plurality of delay elements,
- step control means receiving a next block control signal as input, and
- 35 • sum elements,

000227" FF 2460

5 Hereby, a very simple and efficient implementation of a  
windmill polynomial sequence generator is provided.

This object is achieved by a method of the aforementioned type, said method further comprising the steps of:

- 20 In this way a method is provided which efficiently provides a PN sequence with enhanced unpredictability but with a small additional computational effort.

In accordance with another embodiment, the step control  
30 signal ( $S_t$ ) is provided on the basis of a clock control  
value/signal ( $C_t$ ) and a previously generated select value  
( $M_{t-1}$ ).

In a preferred embodiment, the plurality of sequence  
35 values is two, the step control signal ( $S_t$ ) is calculated

Hereby a  $(1,2)$ -step clock controlled m-sequence generation method is provided with very little additional computational effort.

Hereby an efficient (1,2,3,4)-step clock controlled m-  
sequence generation method is provided which is even more  
15 unpredictable.

Hereby an efficient N-step clock controlled m-sequence generation method is provided which an unpredictability  
25 that grows with N.

30 The present invention also relates to the use of the method and/or electrical device mentioned above in a portable device. In a preferred embodiment the portable device is a mobile telephone.

35 Hereby, efficient and more safe encryption of digitized  
speech may be obtained.

5

10 Figure 1 illustrates a functional block diagram of a  
prior art (1,2)-step clock controlled m-sequence  
generator;

Figure 3 schematically illustrates a combination of a windmill generator and a Clock and Select system (CS system);

Figure 5 shows a preferred realisation of ADD, MOD 2, and  
25 DIV 2 operations in hardware;

30

Figure 8 shows a flow chart of the method according to  
35 the invention;





$$\sigma(t) = \sum_i C_i \quad C_t \in \{1, 2\},$$

5

10

15

30

35

As an example, the initial values shown from left to right (0, 1, 0, 1, 0) will generate the following output sequence  $Z_{2t}(205) = 1, 0, 0, 1, 1, 0, 1$  and  $Z_{2t+1}(206) = 1, 0, 1, 1, 1, 0, 1$  for  $t = 0 \dots 6$ , if the next block control signal (202) is enabled.

15

20

25

30

35

The CS system (301) is responsible for the pacing of the windmill generator (201) by providing the step control signal  $S_t$  (304) and for selecting one of the two output symbols  $X_{2i}$  (302) and  $X_{2i+1}$  (303). The selected symbol is the final output symbol  $Z_t$  (305).

In this way, one cipher of the PN sequence will be generated for each clock cycle. The resulting PN sequence has a high degree of unpredictability since no linear relationship between the output ciphers exists, i.e. either the next symbol or the next symbol again is output. The output is obtained at the same rate as the input clock rate ( $C_i$ ) without the need for multiple clocks and by very little additional hardware.

Figure 4 shows one realisation of the CS system (301) shown in Figure 3. This realisation of the CS system (301) in combination with the windmill generator (201) will result in a (1,2)-step clock controlled m-sequence generator.

Shown is selection means (401) adapted to select one of the two symbols  $X_{2i}$  (302) and  $X_{2i+1}$  provided by the windmill generator (201). The selection is done on the basis of a previously generated select value  $M_{t-1}$  (406)

5

The previously generated select value  $M_{t-1}$  (406) is received from a delay element D (403) which keeps a newly generated select value  $M_t$  (407) for one time instant/clock cycle.

The clock control signal value  $C_t$  (306), pacing the CS system, is added by addition means (402) to the previously generated select value  $M_{t-1}$  (406). The sum (408) of  $C_t$  (306) and the previously generated select value  $M_{t-1}$  (406) can take the values 1,2,3.

From this sum (408) the new select value  $M_t$  (407) is derived by the MOD 2 means (404), i.e.  $M_t$  (407) = ( $C_t$  (306) +  $M_{t-1}$  (406) ) MOD 2, and the new select value  $M_t$  (407) is kept in the delay element D (403), as described above.

30

35

5

10

$C_t$	$C_t^0$	$C_t^1$
0	1	0
1	0	1

20

25

30

5

10

15

20

$$S_t = (C_t (603) + M_{t-1}) \text{ DIV } 4,$$

25

$$M_t = (C_t (603) + M_{t-1}) \text{ MOD } 4.$$

30

In this way a PN sequence with an even larger degree of unpredictability is provided with very little additional hardware.

35

using the same techniques and giving the same advantages as described above.

Figure 7 shows a generalized embodiment of a clock controlled m-sequence generator. Shown are a windmill generator (701) and a CS system (702) which has been generalised to a  $N$ -rate, where  $N$  is at least 2.

The CS system (702) receives the clock control signal value  $C_t$  (703) now  $\in \{1, \dots, N\}$  and the windmill generator outputs  $N$  sequence values/symbols  $X_{Ni}$  (704),  $X_{Ni+1}$  (705), ...,  $X_{Ni+N-1}$  (706) on the basis of the step control signal  $S_t$  (707).

Only one of the  $N$  sequence values (704 - 706) is selected as the final output symbol  $Z_t$  (709) of the PN sequence. The selection of one of the  $N$  symbols (704 - 706) in the CS system (602) is still provided on the basis of a previously generated select value  $M_{t-1}$ .

The step control signal  $S_t$  (707) may be provided on the basis of the clock control signal value  $C_t$  (703) and the previously generated select value  $M_{t-1}$  according to:

$$S_t = (C_t (703) + M_{t-1}) \text{ DIV } N,$$

and the new generated select value  $M_t$  may be provided on the basis of the clock control signal value  $C_t$  (703) and the previously generated select value  $M_{t-1}$  according to:

$$M_t = (C_t (703) + M_{t-1}) \text{ MOD } N.$$

In this way, a PN sequence with an arbitrary large degree of unpredictability is provided with very little additional hardware.



The degree of unpredictability may be chosen according to a specific need for a given implementation.

Figure 8 shows a flow chart of the method according to the invention. The method generates a plurality of PN sequence values/symbols and selects one of these as output.

The method is initialised at step (801).

10

At step (802) a select value  $M_t$  is provided. The select value  $M_t$  may be calculated on the basis of a clock control value/signal  $C_t$  and a previously generated select value  $M_{t-1}$ . The clock signal  $C_t$  may e.g. be provided by an external control method or hardware circuit. The first time a select value is calculated, the previously generated select value may have the initial value of 0 or 1.

15

20 Preferably, the select value  $M_t$  is calculated as  $M_t = (C_t + M_{t-1}) \text{ MOD } 2$  for a plurality of sequence values being equal to two.

Alternatively, the select value  $M_t$  may be calculated as  $M_t = (C_t + M_{t-1}) \text{ MOD } 4$  for a plurality of sequence values being equal to four.

25

Other functions than MOD and DIV and other values than  $C_t$  and  $M_{t-1}$  may be provided.

30

At step (803) a control signal  $S_t$  is provided. The generated control value  $S_t$  is used to control the generation of sequence values at step (804).

5 Preferably, the control value  $S_t$  is calculated as  $S_t = (C_t + M_{t-1}) \text{ DIV } 2$  for a plurality of sequence values being equal to two.

10

15

20

25

30

5 At step (805) one of the plurality of generated sequence values is selected and output as the next symbol in the output PN sequence. Preferably, the selection is done on the basis of the select value  $M_t$ . This selection of a value between a plurality of uncorrelated sequence values greatly enhances the unpredictability of the output sequence.

In this way, a higher degree of unpredictability is obtained by very little computational effort.

30

35 Figure 10a shows a communications system (1001)  
comprising a first transmitting/receiving station (1003)

and a second sending/receiving station (1004) where information (1005) may be transmitted. The PN sequences generated by a (1,2)-step clock control m-sequence generator of an embodiment of the present invention may be used as a sub-component to encrypt information (1005) to be transmitted between the first transmitting/receiving station (1003) and the second transmitting/receiving station (1004).

Alternatively, a quaternary-rate (1,2,3,4)-step clock controlled m-sequence generator or other rate generators, as described in connection with Figures 6 and 7, may be provided in the system to improve the unpredictability even further.

In this way, safe transmission of information (1005) like data, digitized speech signals, etc. may be achieved by using less hardware, thereby reducing the costs and power consumption.

Figure 10b shows a transmitting/receiving station (1003) and a mobile terminal (901) which form a cellular communications system (1002). The information (1005) to be transmitted/received between the mobile terminal (901) and a network infrastructure (not shown) via the transmitting/receiving station (1003) may be encrypted through the use of a ciphering system that uses PN sequences generated by multi-rate clock controlled m-sequence generators.

Alternatively, a quaternary-rate (1,2,3,4)-step clock controlled m-sequence generator or other rate generators, as described in connection with Figures 6 and 7, may be provided in the system to improve the unpredictability even further.

5